actor based on outputs from the one or more application software program modules **142**.

[0022] FIG. **2** is an exemplary illustration of a data structure for a role assignment record **200**. The role assignment record **200** is one of the entities upon which authorization can be determined by the system **100**. A role can represent a named container in which to assign one or more actors who, for example, can have a set of common attributes and/or a set of common permissions and capabilities. A role can be a link between actors and policy instances that enables role-based authorization. An actor can have one or more roles, and a role can have one or more actors associated with it. For example, an actor might be an employee, a manager, and/or employee benefit plan participant. In such examples, an application can use any or all of these assigned roles, however, only one of the actor roles may be in effect at any given time within the application. In such examples, the user either explicitly selects a role or the application implicitly selects a role based upon the workflow context.

[0023] Roles can form a hierarchy whereby a role can inherit and extend the permissions of another role. Associated with a role are one or more policy instances that, in conjunction with the scope associated with the role of a user, specify which resources the actor can access and the extent of the resource access. Role assignment is based, in part, on one or more context parameters. For example, an actor has the role of "manager" based upon the fact that a given business entity employs the actor in a managerial capacity within a given organization (e.g., the organization being an exemplary context parameter). Alternatively, that same actor can have the role of "plan participant" if the actor is, for example, acting in the context of an organization that is a client to a retirement or benefits plan administrator (e.g., communicates with the system through a Web interface for the particular retirement plan).

[0024] Role assignment includes the creation of a role assignment record **200**. A role assignment record includes, for example, an actorID **202***a*, the name of the role **202***b*, context parameters **202***c*, and a actor-role scope **202***d*. The actorID **202***a* is the identity of the user, system account, system application, batch process, or other computing device assigned to the role. The name of the role **202***b* can be specified during the role set-up or administrative process. Role names can include, for example, "manager," "employee," "plan participant," "system administrator," and the like. Context parameters **202***c* are variables that make the role assignment unique to the actor. Context parameters can include, but are not limited to, parameters such as "client identifier," "practice identifier," "plan number," "product identifier," "market segment," and "authentication strength." For example, a user named "Bob" is assigned to the role of "manager," and has a context parameter of "client." In another example, the user named "Bob" is assigned the role of "brokerage customer" where the context parameter is "account type."

[0025] The role assignment record **200** can also include a actor-role scope **202***d*. The actor-role scope **202***d* includes a key that allows a consuming system and/or application to obtain the resolved scope of action that an actor is permitted to perform. The actor-role scope **202***d* includes one or more values applicable to a given role assignment for an actor. The actor-role scope **202***d* of the role assignment record **200** is derived from a role scope **208** by taking into account one or more pre-defined context parameters specific to an actor. A role scope **208** includes a general specification of the scope of authorized action for an actor, e.g., the definition of who and/or what can be acted upon by an actor in a particular role. For example, a role assignment record **200** can include an actorID **202***a* for the user "Bob" who serves in a role named **202***b* "manager" in the context **202***c* of "ABC Client Corporation." The actor-role scope **202***d* of the role assignment record **200** in this example is determined based on the role scope **208**. In this example, the role scope **208** includes "department name." This means that during the assignment process of the user **110**, "Bob," to the role named **202***b* "manager," a department name is required to resolve the scope of the "manager" role. In this example, the actor-role scope key **202***d* enables resolution of scope that includes, for example, the "purchasing department" for the department name.

[0026] Some other examples of data that can be included as role assignment elements in the role assignment record **200** are start/end date for the role, assignment status, e.g., active role available for assignment, inactive role that cannot be assigned, role grantor or proxy, owner of the role who can be responsible for definition and maintenance of the role and associated policies, a list of consumer applications that can use a given role, role assignment rules, e.g., rules related to the mutual exclusivity of particular roles for a given user, and the like.

[0027] FIG. **3** illustrates a process flow diagram **300** for role-based access in a multi-customer computing environment. In the diagram **300**, the user **110** (one type of actor) logs on (**301**) to a computer system by providing, for example, a userID and password. The identity of the user **110** is established through system verification of the authentication credentials that the user inputs into the system **100**. If the user **110** is authenticated (**302**) by the system, then one or more pre-defined context parameters are obtained (**303**).

[0028] Context parameters can include one or more attributes that describe, for example, the manner and circumstance in which an actor can interact with one or more given resources. Context parameters include, for example, role-related context parameters, session-related context parameters, and/or any combination thereof. Role-related context parameters play a part in the assignment of roles, the management of policies, and the selection of policy instances. In some examples, role-related context parameters may not relate to the runtime environment of the application consuming the policy instance data. The reason for this is that actor-to-role assignment, in some examples, does not depend upon runtime factors. In such examples, the one or more pre-defined context parameters associated with role assignment focus more on organizational factors, e.g., the division in which a user is employed. Session-related context parameters can include parameters related to the interactions of the actor with a computer system. The session-based context parameters can include, but are not limited to, parameters associated with one or more consuming applications (e.g., applications that are requesting access to one or more resources), one or more points of claim, which can relate to the one or more sources of consuming application usage, alternative user authentication mechanisms and strengths associated with various access paths to one or more applications, date and/or time ranges associated with one or more policy instances, and/or any combination thereof. In some examples, session-related context parameters can be hierarchical in nature. For example, such a